IT Outsourcing

End User Services and Network & Security Infrastructure Statement of Work / Supplemental Agreement SAMPLE

GLOBAL IT OUTSOURCING

Sample Prepared for:

<DIR Customer>

Date:	Month, Day, 2007
Document Description:	End User Services and Network & Security Infrastructure Statement of Work / Supplemental Agreement ***SAMPLE***
Revision:	0.3

Trademarks

Table of Contents

1 Introduction

1.1 Engagement Overview

Unisys is pleased to offer this ITO Statement of Work to serve as the "Supplemental Agreement" to <DIR Customer> to support its Seat Management needs. This document details the Unisys Services ("Services") that are provided through a combination of personnel and tools deployed at major <DIR Customer> site(s), those deployed at remote <DIR Customer> sites, and those deployed in the Unisys Managed Services Centre (MSC).

Unisys shall provide to <DIR Customer> the following Services set forth in this ITO Statement of Work, or as otherwise agreed to in the Change Management process:
The Unisys solution is comprised of the following key components:

- **Managed Procurement Services** – Unisys will enable DIR's Customers to efficiently evaluate, source and track a wide variety of IT products. Primary functions include ordering, approvals, fulfillment, shipment, tracking, installations and returns. Unisys Service is an integrated manufacturer-independent solution
- **Single Point of Contact (Service Desk) –** Unisys will provide a Single Point of Contact for all support services provided by Unisys. We will deliver Service Desk support to the end users from our multi-channel, first-line support desk in Austin, Texas. Staff in the Service Desk will be responsible for resolving, managing, routing, tracking and escalating all support tickets, using a single ticketing system
- **Desktop Management** – Unisys will the building, testing, and distributing consistent images of workstation software for the DIR's Customer's end users. Unisys is completely responsible for managing all aspects of software licenses, regardless of software vendor.
- **Mobility Management** – Unisys leverages more than 20 years of experience in managing mission critical applications associated with a mobile infrastructure. We have key partnerships with Microsoft, Nokia, Intellisync, and Dexterra to manage and control a mobile infrastructure, which includes hardware, software, deployment, and installation management and control.
- **On Site Support and Moves, Adds and Changes (MACs) -** Unisys will use a combination of dispatched and dedicated resources to deliver the required onsite and MAC support. We will leverage both our dedicated and shared resources to deliver the support services to the end users across the state of Texas, therefore reducing the cost for onsite support
- **Device Monitoring and Management -** All distributed server, storage, network, firewall and other elements of the enterprise will be monitored and managed from our Managed Service Center located in Austin, Texas. We will use the Unisys Managed Service Center in Austin, Texas as our primary support location and our center in Egan, Minnesota as a backup center. Unisys will ensure 24x7 support services are available to identify and solve system problems. Support for management and operation of storage systems, technology platforms, operating

systems and databases will be provided by teams of engineers with platform or application expertise from our Global Support Centers. Other support staff will be distributed to locations where local support is necessary

- **Break-fix / Maintenance –** Unisys provides comprehensive multi-vendor service offerings for distributed computing environments. We will effectively maintain and manage all multi-vendor IT infrastructures by providing a single-vendor model for comprehensive support across desktops, servers, networks, and software.
- **Asset Management –** Combining Service Desk automation with IT asset management automation provides a great deal of time during the problem resolution process. By automating multiple asset management functions, we are able to provide real time information to speed up problem resolution, ensure data accuracy, and decrease incident management costs
- **Service Management –** To manage all aspects of the overall service, Unisys will establish and maintain a Program Management Team, staffed with experienced IT professionals, to deliver operational excellence on an enterprise-wide scale. Leveraging our experience in vendor management, this Team will also be responsible for providing all third-party vendor management services

Before the full service can begin, an Implementation project is required. Here, key Unisys and <DIR Customer> personnel team together to document the business and technical information required to clearly define the steps required to initiate service. The solution previously defined in the Engagement phase is then modified as necessary, utilizing the mutually agreed to SOW Change Management Process, and deployed.

After the Implementation project is complete, the contracted services are provided for the length of the contract.

1.2 Service Overview

The following graphic shows the interrelationships between the services
NOTE: ***This will be designed and placed in this area based upon the suite of services ordered by the DIR Customer.***

2 Services to be delivered

2.1 Managed Procurement Services (also know as Provision of Equipment and Procurement Services)

2.1.1 Service Definitions

Unisys will enable DIR's Customers to efficiently evaluate, source and track a wide variety of IT products. Primary functions include ordering, approvals, fulfillment, shipment, tracking, installations and returns. Unisys Service is an integrated manufacturer-independent solution. The intent of the Master DIR Agreement DIR-SDD-537 is not for procurement of commodities, but as procurement for services.

2.1.2 Managed Procurement Services Terms and Conditions

Managed Procurement Services/Provision of Equipment and Procurement Services: Customer and Unisys will agree to the terms and conditions for this Service, (including provisions that will protect Unisys rights and interests in relation to the equipment provided to a Customer), in the mutually agreed upon Statement of Work/Supplemental Agreement for the contracted services.

2.2 Service Desk

2.2.1 Service Definitions

Unisys will provide a Single Point of Contact for all support services provided by Unisys. We will deliver Service Desk support to the end users from our multi-channel, first-line support desk in Austin, Texas. Staff in the Service Desk will be responsible for resolving, managing, routing, tracking and escalating all support tickets, using a single ticketing system. The Unisys Service Desk Service provides <DIR Customer> with a full portfolio of hardware and software support via phone, email and Unisys Service Portal. The service desk is the single point of access and control, ensuring proactive, monitoring, escalation, and service request and incident resolution.

The Unisys MSCs will receive calls for incidents and service requests and will enter them into the Incident Management System, record the issue according to incident or request and will manage the issue to resolution.

Unisys will be supporting, for <Client's> environment, the following types of end users:

NOTE: ***This will be placed in this area based upon the level of service ordered by the DIR Customer.***

Unisys responsibilities include:

NOTE: ***This will be placed in this area based upon the level of service ordered by the DIR Customer.***

<DIR Customer> responsibilities:

1) Communicate the new features of the Service Desk to end users.
2) Provide initial information for incident management system, as defined below:
   End User Data Load
   a. Typical information required: Personal End User Data: Last Name, First Name, Phone Number, Unique ID, E-Mail Address
   b. Address Data: Location, Street, City, State, Zip or Postal Code, Country
   c. Asset Data: PC Asset Tag, Make, Model, Serial Number
   d. Unique ID of End User associated with the device * (must map to End User Unique ID provided in End User Database)
   e. Location of the Device *
   f. Asset Tag
   g. Cost Center for the Device
   h. Internal and 3rd party Resolver Groups, group members, supported applications

   *Required Asset Data

3) The Client shall provide individual User updates (additions, deletions, changes) on a regular basis.
4) For any new systems, the Client shall supply a complete list of hardware and software deployed, with resolver groups for each
5) Trouble-shooting scripts and referral requirements
6) For any new supported item, the client shall provide a description of the application, frequently asked questions with answers, common problems with resolutions and information to be collected from the User prior to referring a ticket to a resolver group.
7) Provide updated information on an agreed to frequency, as defined above
8) Training
    a. Client shall be responsible for training End Users in the use of the Standard Operating Environment (SOE) and associated applications.
    b. Client shall provide training to Unisys' Service Desk Trainer(s) on the Client applications and all supplied knowledge base and procedures documentation.
    c. Client shall be responsible for the shipping of all equipment de-installed and requiring relocation to another facility

2.2.2 Incident Management

2.2.2.1 Incident Recording:

The goal of incident management is to restore normal service operation as quickly as possible with minimum disruption to the business, thus ensuring that the best achievable levels of availability and service are maintained.

For Incident Management activities, Unisys responsibilities include:

1) Act as the single-point-of-contact for all IT-related User calls;
2) Accept User calls by telephone, email and Self Service Web portal.
3) Validate User entitlement for Service;
4) Create a Service Management Record for every User call, whether by telephone, email or Self Service;
5) Handle all enquiries to the Service Desk from Users including those that may not be concerned directly with the Services.

2.2.2.2 Classification and initial support:

1) Classify, prioritize, refer, track and escalate User incidents, based on the severity chart below.

Severity	Definition – GLOBAL LIST
1 - Critical	Severe Business Disruption
2 - Major	Major Business Disruption
3 - Medium	Minor Business Disruption
4 - Low	Minor Disruption
5 - Very Low	Inquiry

2) Match incidents against the published list of problems and known errors and, where a known error is found, pass the details or work-around to the User.
3) Maintain a current and historical Record log of all incidents.

2.2.2.3 Investigation and diagnosis:

1) Obtain and record the required referral information, as defined by each resolver group.
2) Assign the incident to the appropriate resolver group, based on agreed referral rules.

3) Issue the End User with a unique reference Record number for each incident not resolved on the initial contact with the End User.

2.2.2.4 Resolution and Recovery:

1) Classify and close all incident Records resolved on the initial contact with the End User.
2) Classify and close all referred incident Records once the assigned resolver has updated the incident Record as 'resolved', ensuring resolution details and Customer acceptance of resolution are complete.
3) If resolution of the Incident is outside of the Service Desk scope of responsibilities, the Incident will be dispatched or referred to the appropriate resolver group. The Unisys Service Desk will maintain the Incident in an "open" status until the Incident is resolved and closed by the <DIR Customer> resolver group.
4) The ownership, monitoring, tracking and communication process includes managing the Incident Escalation process. All open Incidents are tracked at the Service Desk against Unisys SLAs and client provided OLAs for <DIR Customer> Resolver groups or 3rd party vendors.

2.2.2.5 Incident Co-ordination

Unisys responsibilities include:

1) Act as the co-ordination point between the User and resolver groups during diagnosis, resolution and closure.
2) Monitor all incidents and enquiries for Service Level and relevant KPI compliance.
3) Use mutually agreed escalation time frames and automated notifications (email or SMS text or pager) to alert resolvers of incidents that are about to surpass a resolution threshold.
4) Provide a contact telephone number, which shall route directly to the Incident Coordination Team, for use by <DIR Customer> IT staff and all resolver groups.
5) Provide service outage notifications as appropriate to all Users via a bulletin message on the incoming Service Desk telephone line and web portal.
6) Act as the co-ordination and communication point between Unisys, Customer and resolver groups during Incidents or outages.
7) Initiate and participate in "Major Incidents" according to the process defined by <DIR Customer> and Unisys
8) Act as the coordination point for incident, enquiry, error and problem control.

<DIR Customer> responsibilities:

<DIR Customer> shall provide names and contact details for incident coordination staff within the Client's and third party resolver teams.

Define the "Major Incident" process with Unisys.

2.2.3 Problem Management

Problems in an IT Service do not always cause disruption, particularly if there has been a temporary fix to an incident leaving an unresolved problem with the service. Identification of a problem in this manner is reactive.

2.2.3.1 Scope

a) Unisys shall identify, track, escalate and coordinate the resolution of Problems that result from IT Services provided by <DIR Customer> and/or its service partners.
b) Unisys shall provide problem resolution and management of Problems resulting directly from the Unisys's scope of services.

2.2.3.2 Pro-active

a) Identify proactively through trend analysis, underlying Problems that are a cause of Incidents.
b) Manage resolution of Problems as defined in Service Scope above.
c) Highlight User training and education needs.
d) Generate a Change Request for those Problem Resolutions that require changes to the infrastructure.

2.2.3.3 Reactive

Unisys is responsible for Managing problems that involve more than one supplier to provide a point of escalation and focus to create a clear action plan to minimize disruption to the User. The Client and its service partners shall participate in this process in accordance with their obligations.

2.2.4 Service Request

Service Requests can be made over the phone to a Service Desk agent or self-logged using a web-based catalog of pre-approved services from which an end user can select. These services may vary from moving a piece of desktop equipment to provisioning a new employee, requiring a desktop build, or requesting password setups.

Services Catalog
The Web based Service Catalog consists of a single, generic online catalog. This catalog includes <DIR Customer> approved generic descriptions of hardware, software and related services .

The Service Catalog items are categorized by standard type (i.e. “standard desktop, standard laptop, standard printer, standard office suite software, standard PDA”, etc). Manufacturer and/or part numbers are not included.

The Service Request Process does not include external integrations with ERP system, vendor or 3rd party systems.

Bundles of products and services will be developed based on the request types as listed below in section 2.1.4.1

Unisys Responsibilities:

1) Unisys shall develop and maintain, in close cooperation with the Client, an electronic Services Catalog of agreed items, which includes:
    a. a) The Client’s Standard products
    b. b) The range of services available to the Client Users
2) Unisys shall make the Services Catalog available to the Client Users via the Request Management System.
3) Unisys shall be responsible for all aspects of Request Management System functionality.

<DIR Customer> Responsibilities.

1) The Client will submit Catalog updates will be based on changes submitted through the approved change process.

2.2.4.1 Request Types

1) Unisys shall manage the requests via the Request management system with the following Standard Request Bundles

    NEED TO DISCUSS SCOPE ISSUE
    On-boarding New Employee

- Standard Desktop
- Standard Laptop
- Telephone
- Email

Telecoms

- Voice Provisioning (includes handsets, PBX or Centrex Services)
- LAN Services
- WAN Network services (as specified by <DIR Customer>)

New Hardware Request Bundle

- Standard Desktop (including printers)
- Standard Laptop

New Software Request

- Standard Software
- Non-Standard Software

Move Hardware

- Standard Laptop
- Standard Desktop
- Telephone

De-install Hardware Request

- Standard Laptop
- Standard Desktop
- Telephone

De-install Software Request

Off-boarding User Request

- Remove Domain / Intranet Permissions
- Remove Intranet Permissions
- Remove Share Access
- Remove VPN Account
- Remove Additional System Access

Add/Modify Permissions

- Network
- File sharing
- Local File/print, Email, FAX and Internet Access services
- Local Active Directory/DNS/DHCP services

Unisys and the <DIR Customer> will work together to identify current processes and tasks associated with the ten (9) types of requests as listed above. Based on best practice, Unisys will then compare and contrast to the processes and tasks built into the solution. Each process typically starts with the end user requesting products and services within the Request Management system and moves through to the Unisys backend workflow engine where the request will be fulfilled.

2.2.4.2 Request Authorization

The End User shall select the required product or service to be delivered from an approved list located within the Request Catalog. At this time they will be assigned a unique reference number for their request.

The Request Management System shall automatically send notification of the request via e-mail to the appropriate <DIR Customer> representatives for approval using a set of operational or financial parameters.

Once approved, requests will be fulfilled based on agreed to processes and tasks associated with the specific request.

Request Status
For requests in the Request Management system, the track request feature allows users to check the status of their requests submitted through the service portal.

Users can check the status of requests submitted by them. <DIR Customer> Users shall use the Request Management System as the prime source for checking their own request status.

<DIR Customer> Responsibilities include:

1) <DIR Customer> shall work with Unisys to agree and maintain a current Supply Catalog.
2) <DIR Customer> shall be responsible for providing details of service provider groups from within its own organization and 3rd party suppliers to populate the Supply Catalog.
3) <DIR Customer> shall provide a set of operational and financial parameters to use for the purpose of request authorization.
4) <DIR Customer> Users or their representatives shall be responsible for the generation of procurement and service requests for those items covered by the Supply Catalog.
5) <DIR Customer> shall be responsible for settling vendor invoices.

2.3 Product Build and Configuration

1) Unisys shall maintain details of agreed to current product builds and configurations within the Service Catalog.
2) Unisys shall ensure that the manufacturer builds and configures product in line with order.
3) New products supplied shall be asset tagged in accordance with the agreed list of Configuration Items.
4) Unisys will provide the administration function to maintain the Catalog based on additions, deletions, and/or changes provided by the Client.

2.3.1.1 Logistics

Unisys shall be responsible directly, or via the product manufacturer, for the logistics of delivering the product to the required location in line with the request.

2.3.1.2 Status and Escalation

1) Unisys shall update the Request Management System with agreed status points in the life of each Request up to and including request closure.
2) Unisys shall provide an on-line status enquiry capability to allow the requester to determine the status of their own requests in the request management system.
3) Unisys shall provide an on-line status enquiry capability to allow the client's Service Manager to determine the status of any request in Unisys's process.
4) Unisys shall track and escalate requests in line with the Service Levels.

2.3.2 IMACD

2.3.2.1 Pre-IMACD Activities

1) Wherever possible Unisys shall pre-configure the requested components prior to installation.
2) Unisys shall receive or organize receipt of products to be moved to or installed at the installation location.
3) Unisys shall check the requested installation site for appropriate power, LAN connectivity, cables etc. Where it is impractical to undertake this activity prior to installation, then it shall form part of Unisys's on-site activities.
4) Where the IMACD activity cannot proceed as a result of the above check, Unisys's Technician shall refer to Unisys's Service Delivery Manager for appropriate action to be taken.
5) Supplier shall ensure that all new equipment is electrically tested in accordance with local legislation and labeled accordingly.

2.3.2.2 On-Site Activities

1) Unisys shall be responsible for all component installation and de-installation activity.
2) Unisys shall be responsible for managing any dead on arrival (DOA) issues in line with the contract between the <DIR Customer> and the vendor and in accordance with the warranty agreements.
3) Unisys shall be responsible for post installation configuration such as printer set-up.
4) Unisys shall consider an installation complete once the User is able to use the device being installed.
5) Unisys's technician shall provide such details of IMACD completion to enable Unisys's Request Management Team to register the Request as complete.

2.3.2.3 Post IMACD Activities

1) Unisys shall be responsible for removing redundant equipment from site into Unisys's temporary storage location as provided by the client
2) Unisys shall be responsible for the disposal or re-distribution of any redundant <DIR Customer> owned equipment in accordance with the procedures agreed and documented with the <DIR Customer>.
3) Unisys shall liaise with any equipment owner regarding the disposal or re-distribution of any redundant equipment not owned by the <DIR Customer> but shall not be responsible for any disposal, re-sale, or income distribution.
4) Unisys shall be responsible for any de-commissioning and data removal from all redundant hard disks prior to disposal or re-distribution.
5) Unisys shall be responsible for packaging and disposal of all equipment associated with the delivery of the <DIR Customer> components in line with local regulatory requirements..

2.3.2.4 Project Based IMACDs

Requests in excess of 5 devices shall be treated as projects and subject to individual arrangements and quotation.

2.3.3 Supported Software Products

Software applications supported by the Unisys Service Desk will fall into one of the two following categories:

2.3.3.1.1 Category 1

This category shall consist of the Desktop Standard Software Suite Applications. Some of the more common packages include but are not limited to the following:

Supported Work Station and Laptop Software

Note: Will be determined based upon the level of service contracted by the Customer from the Service Levels Proposed

2.3.3.1.2 Category 2

This category shall consist of <DIR Customer>'s Proprietary Applications and <DIR Customer> Server and desktop applications listed in Cost Model.

1) Unisys will provide Level 1 Support per <DIR Customer> provided training, documentation and scripts.
2) <DIR Customer> will provide Level 2 Support for these applications.
3) Unisys will monitor and escalate the Incident with <DIR Customer> and or the named <DIR Customer> third party resource until the Incident is resolved.

2.3.3.1.3 Category 3

The Unisys Service Desk will refer Incidents to the appropriate <DIR Customer> resolver groups for proprietary application calls that cannot be resolved by the Unisys Service Desk.

2.3.4 Customer Satisfaction and Complaint Handling

2.3.4.1.1 Customer satisfaction surveys:

To measure End User satisfaction, Unisys conducts point-of-service surveys via e-mail to measure the qualitative elements of the service delivery. Surveys are conducted on approximately 10% of the closed Service Desk resolved Incidents for the prior month.

2.3.5 SLAs and KPIs

For SLA's please see Appendix E

2.3.6 Reporting

For Reports please see Appendix F.

2.4 Desktop Management

2.4.1 Service Definitions

Managed Desktop Services (MDS) offering is comprised of the following service elements:

- Inventory Tracking
- Electronic Software Distribution
- Security Patch Management
- Software License Administration (optional)
- Image Management (optional)

2.4.2 Inventory Tracking

Unisys Responsibilities include:

1) Unisys shall create an initial baseline inventory repository, which will be populated with a combination of existing client information and auto scan information
2) If client does not have an existing device inventory, Unisys shall provide a physical inventory of the client's IT infrastructure as an optional service for an additional charge.
3) Unisys shall provide tracking of agreed-to <DIR Customer> hardware and software inventory associated with the IT Services, including;
    a. Receiving Devices for <DIR Customer>, and recording the devices in the Inventory repository.
    b. Maintain Unassigned inventory
    c. Track recycle inventory
    d. Track inventory to be disposed
4) Unisys shall update the Inventory data as a result of the Field Support activity, IMACD, and requests.
5) Unisys shall update the Inventory database as a consequence of approved changes to Configuration Items or valid change management.
6) Unisys shall develop a rouge device capture process

<DIR Customer> Responsibilities include:

1) <DIR Customer> shall provide Unisys with an existing device inventory to be used in populating the baseline repository.
2) <DIR Customer> shall provide Unisys with required access to carry out periodic physical checks of the inventory base.
3) Unisys shall not be responsible for changes to hardware and software inventory made directly by <DIR Customer> Users and/or service partners, outside of the agreed Request Management and Change Management procedures.
4) <DIR Customer> shall be responsible for developing and maintaining its internal financial asset database.

2.4.3 Electronic Software Distribution

Unisys Responsibilities include:

1) Unisys will distribute Software in response to a single end user request or in response for software to be distributed to a group of users.
2) Software distribution requests will be received as tasks from the Unisys Service Request Management.
3) Unisys will prepare a Software Distribution Package to a certified software application package in response to requests if a distribution package does not already exist during steady state operations

<DIR Customer> Responsibilities include:

1) <DIR Customer> shall provide Unisys with its plan for new applications development and agree a plan of any new requirements.
2) <DIR Customer> IT management and requesting Users shall work with Unisys to develop a full understanding of Non Standard Solution business requirements.

2.4.4 Security Patch Management

Unisys Responsibilities include:

1) On a weekly basis, Unisys will retrieve a list of newly available patches and provide analysis of PCs at risk to the Unisys PMO for submission to the Change Advisory Board.

2) Unisys will set up the security patch delivery method and schedule the distribution per approved change request.

<DIR Customer> Responsibilities include:

1) <DIR Customer> shall provide an Anti-Virus tool compatible with the <XXX operating system> environment for all servers, desktops and laptops.
2) <DIR Customer> provided Anti-virus tool shall be capable of notification of successful deployment for Anti-Virus signature updates.
3) <DIR Customer> shall mandate that its third parties and other Partners who may utilize the Client network, are in compliance with the agreed virus management policy.
4) <DIR Customer> will determine which Patches to apply and the urgency (Emergency or non-emergency).
5) <DIR Customer> Security group and or other <DIR Customer> resolver group will evaluate and test patches and communicate results of testing to Unisys.

2.4.5 Software License Administration

Unisys Responsibilities include:

1) Unisys will upload the software license details into the Definitive Software Library (DSL).
2) Unisys will provide monthly application license usage and compliance reporting as generated from inventory scans monitoring the operating system for application launch and termination events

<DIR Customer> Responsibilities include:

1) <DIR Customer> will provide software license details to include, but not limited to application name, alias, version number or suite name and version, license quantities, license numbers, manufacturer, purchase date, and other details as mutually agreed to.
2) As purchases are made, <DIR Customer> will provide updated license details in a mutually agreed to electronic format.

2.4.6 Image Management

Unisys Responsibilities include:

Unisys will provide Image Management services to <DIR Customer> based on assumptions made to the number of configurations and images as follows:

1) Unisys will participate in the change management process to test new technology as a result of change requests submitted to the CAB
2) Unisys will test and certify new applications or hardware drivers against the existing core image per test scripts mutually agreed to during the implementation
3) Unisys shall test software builds intended for use within the Standard Operating Environment (SOE), and work with the technical support staff of <DIR Customer> and its partners to resolve any incidents noted.
4) Unisys shall provide advice and input to new requirements for the SOE arising from any applications developments. <DIR Customer> shall provide Unisys with its plan for new applications development and agree a plan of any new requirements for the SOE.
5) Unisys shall develop standard image builds, deployment scripts, image version control and compatibility testing with hardware and software SOE and the <DIR Customer>'s software.
6) Unisys shall manage and maintain a library of image builds
7) The Unisys will be responsible to maintain <DIR Customer>'s existing Image per mutually agreed to CAB change requests.

<DIR Customer> Responsibilities include:

1) A list of <DIR Customer>'s current software will be maintained by <DIR Customer> and be available to Unisys.
2) <DIR Customer>'s current software will be maintained by the Client and be available to Unisys.
3) <DIR Customer> will provide Image Server(s) as required
4) <DIR Customer> is responsible for strategic Image decisions that include, but are not limited to:
    a. Definition of the Core Image (e.g. Windows vs. MacIntosh, MS Office XP Profession vs. Standard, Outlook vs. Lotus Notes, Desktop and Laptop hardware standards)
    b. Other COTS (common off the shelf) applications (e.g. Vision, Project)
    c. Enterprise applications (e.g. SAP vs. PeopleSoft)
    d. Client developers will validate the certification of applications against the Client's proprietary applications

2.5 SLAs and KPIs

For SLA's please see Appendix E

2.6 Reporting

For Reports please see Appendix F.

2.7 Technology

2.7.1 Incident Management System

Unisys utilizes an integrated support systems to manage <DIR Customer> Incidents, Service Requests, and the <DIR Customer> services described in this SOW. The Unisys Incident management tool will be the primary repository for entering Incident and Service Request data and gathering service level performance metrics

2.7.1.1 .<DIR Customer> Access to the Incident Management System

Unisys will provide <DIR Customer> with 15 concurrent accesses to the Unisys Incident Management System for the <DIR Customer>'s 2nd and 3rd level support employees to be able to review, update and close Incidents referred to them from the Service Desk. Each access support creation of up to ten (10) logons. Unisys will provide pricing to <DIR Customer> if additional accesses are required.

2.7.1.2 Service Portal

Unisys will provide and support multi-lingual self service access to Service Portal. The Service Portal is a pre-designed and configured Unisys tool linked to the Incident Management System. The Service Portal will be personalized for <DIR Customer> to include logo and client specific home page copy per Service Portal available personalization sections. The Service Portal provides for:

- Home Page news items and service updates,
- End User Incident Submission and access to view current and previous Incidents,
- End User access to submit Service Requests and view Request status,
- End User access to self help support tools,
- <DIR Customer> and Unisys PMO access to management reports.

Unisys Service Portal is a web based tool with secured, password protected logon controlled by data - within the Incident Management System setup and access rights created for <DIR Customer> Management access to management reports.

End Users may select from one of the following Service Portal languages:

- Dutch
- English
- French
- Italian
- Portuguese
- Spanish

Service Portal self service content is geared to address the support requirements of End Users. Unisys and <DIR Customer> will mutually agree to End User appropriate FAQs and <DIR Customer> specific knowledge base solutions.

- Unisys will post <DIR Customer> specific FAQs and knowledge base solutions that are provided by <DIR Customer>.
- <DIR Customer> will provide translations of FAQs and knowledgebase solutions in all supported Service Portal languages.

2.7.2 Knowledge Base

1) Unisys is responsible for creating and maintaining an English language knowledge base containing the client's system and application information in order to assist in resolving incidents and enquiries.
2) Unisys, the Client and 3rd party suppliers shall supply the knowledge articles and work-a-rounds to populate relevant sections.
3) Maintenance of the knowledge based system is linked in with other program controls, e.g. change management and problem management.
4) Customer Users, licensees, and agents will have web access to the Self Service Portal.

2.8 On-Site Support Services

Note: Unisys will provide On-Site Support Services delivery based on the SLA's outlined in the Proposal

2.8.1 Infrastructure Maintenance Service Definition & Description

The Infrastructure Maintenance Services will provide the following IT Infrastructure Support and maintenance functions:

- Hardware Maintenance
- Deskside Software Support
- Installations, Moves, Adds, Changes, and De-Installations

On-Site Support Services are defined as the local operational support and management of the devices Distributed IT Infrastructure environment, at the <DIR Customer> Sites listed in the enclosed Client Site List in Appendix L. Such Services include the support of end-user devices as defined in appendix A. Unisys is responsible for the work performed and for meeting the requirements of the Service Levels as defined herein.

On-Site Support Services shall consist of the services set forth below.

The Unisys Service Desk will create an On-Site SR (Service Request) within the Incident Management System for the dispatch of Unisys supported hardware. This will systemically

create a service ticket in the Unisys dispatch application where additional triage, part ordering, and notification to a service technician occur. See Appendix G for a list of the Unisys Supported Hardware.

Hardware that is defined as supported by a <DIR Customer> resolver group will be referred within the Incident Management System as previously described.

Hardware supported by a third party vendor will require a Letter of Agency to allow Unisys to dispatch. When on-site service is required, the Unisys Service Desk will contact the respective service provider on behalf of <DIR Customer> with specific device information. Unisys will request status updates and, if the third party service provider provides these updates, the Service Desk will include these updates in the Incident ticket work-log.

2.8.2 Hardware Maintenance

Unisys will provide multi-vendor hardware maintenance and support for devices hardware products, including PCs, laptops, printers, and other PC peripherals listed in the enclosed supported products list in Appendix G.

IT Infrastructure Support and maintenance will be provided by the dedicated on-site or dispatched <DIR Customer> Service Representatives with the correct skill level for the problem. Unisys provides the support services that are required in most geographic areas. In less populated areas, Unisys may choose to subcontract support using a third-party service provider that is established within the area. Unisys manages the service delivery using standard call management, dispatch, and logistics systems.

2.8.3 Deskside Support Software

For those support issues not resolved by the Unisys Service Desk on-site deskside software support will be provided. Please see Appendix G for the products that are supported at sites listed in Appendix L, for <DIR Customer> sites that are supported. When deskside software support is required, a Unisys Client Infrastructure Representative (CIR), with the appropriate skill level, will be dispatched to the end-user location to perform software diagnosis and problem resolution.

Unisys can provide an on-site technical resource to:

- Assist in implementing software corrective actions in those cases where the end-user has been unsuccessful under the direction of the Service Desk.
- Perform software diagnostics on behalf of the end-user in those instances where the end-user has been unsuccessful under the direction of the Service Desk.
- Obtain and relay information to a centralized support facility in those cases that the end-user lacks the technical knowledge to do so.

2.8.4 Installations, Moves, Adds, Changes, and De-Installations (IMACD)

IMACDs occur either as ad hoc requirements or as planned, large-scale projects. Unplanned or day-to-day IMACD activity is handled in the same manner as hardware service Requests with call placement utilizing the standard service Request process, that is, individual Requests for IMACDs go through the Service Desk.

All complex Devices and/or large-scale projects (IMACDs greater than 5) are scheduled and coordinated with the Unisys PMO as a project. A Unisys Project Manager is assigned to work with <DIR Customer> on the IMACD implementation. This individual provides scripting or a

complete ITO Statement of Work jointly developed with <DIR Customer> detailing the IMACD activity, including the process for verification of operation of the installed or upgraded device. All pricing associated with this type of project based IMAC activity will based on the rates enclosed in the mutually agreed upon Infrastructure Maintenance Services Resource pricing matrix. This process is communicated to all Unisys service representatives delivering the IMACD service, which results in a consistent, repeatable service execution.

2.8.4.1 Installations

Prior to an actual installation, the Unisys Request Coordinator will coordinate a site survey to:

- Determine the target location is adequately prepared for trouble free install
- Identify and verify cabling and electrical power
- Document cable/electrical power changes/adds if required
- Communicate site requirements
- Understand and document device connectivity requirements

A Unisys Client Infrastructure Representative (CIR) will perform a site survey and return the completed site survey to the Request Coordinator. Unisys will escalate Site Survey discrepancies, such as power requirements or wiring, to the appropriate departments and follow until resolved. Upon completion of all site survey discrepancies, the Request Coordinator schedules the installation activity with the end-user(s) and the Unisys CIR. Install activities will be performed at <DIR Customer>'s locations during the Principle Period of Maintenance (PPM).

Devices to be installed will be delivered by <DIR Customer> to the installation-site, with physical delivery to a predetermined location inside the building where the devices are to be installed. Upon device arrival at the installation-site, the Unisys CIR will install the device and test for functionality according to the mutually agreed upon script. Installation of a new device will consist of the following tasks:

- Unpack the device
- Connect all components
- Set a network printer address
- Set a network address
- Test for network connectivity
- After connecting to the network, download the user's data files that have been previously loaded to a server that Unisys has access to.
- Determine that the unit will boot to an operating (OS) prompt.
- Obtaining end-user acknowledgment of completion of the task

Unisys will perform checks to verify compliance with the installation procedures. If a problem is detected Unisys will take corrective action according to agreed upon procedures to provide device / system operability. Unisys can perform corrective and out-of-scope actions at <DIR Customer>'s discretion for an additional fee.

The old device de-installation is part of the installation of the new device and will include removal of the old device from the end-user's work area to a predefined location.

2.8.4.2 Moves

Prior to de-installation for the move activity, Unisys will conduct a site survey of the new location. After <DIR Customer> has physically boxed and moved the device to the new location, Unisys will re-install the device and test for functionality, according to the agreed upon script. If a problem is detected by the installer, the end-user will be notified and at <DIR Customer>'s discretion, the installer will make the necessary repairs for an additional fee.

2.8.4.3 Adds

This service is available to install new hardware or software components to existing systems. Unisys will un-box the product, conduct a physical inspection, set up the device, install required software, connect and functionally test the device.

2.8.4.4 Changes

This service is available to replace existing hardware or software components on existing systems. Unisys will un-box the product, conduct a physical inspection, set up the device, install required software, connect and functionally test the device.

Standard procedures for ad hoc, day-to-day IMACD activity include:

- Ask the user to verify the operation of the unit and to sign a work completion form upon completion of the IMACD activity
- Report any installation-related problems to the Unisys Account Manager who will relate it to <DIR Customer>'s Program Manager, both resident within the PMO.
- Use <DIR Customer>-supplied virus detection utilities to scan products for viruses on all IMACD activities that impact the end-user's hard drive
- The Unisys CIR forwards any agreed upon IMACD information to the PMO
- Move the devices on the user's desk, connect the devices to the LAN or telephone line if required, test the devices at the user location for functionality per the mutually agreed upon criteria. Unisys will notify the Service Desk that the move is complete via the "completed call" status entered in the SRMS/ServiceCenter system
- Complete the IMACD call ticket per the call closure procedures

2.8.4.5 Standard versus Project IMACD Activities

Standard procedures for ad hoc, day-to-day IMACD activity include:

- Ask the user to verify the operation of the unit and to sign a work completion form upon completion of the IMACD activity
- Report any installation-related problems to the Unisys Account Manager who will relate it to <DIR Customer>'s Program Manager, both resident within the PMO
- Use <DIR Customer>-supplied virus detection utilities to scan products for viruses on all IMACD activities that impact the end-user's hard drive
- The Unisys CIR forwards any agreed upon IMACD information to the PMO
- Move the devices on the user's desk, connect the devices to the LAN or telephone line if required, test the devices at the user location for functionality per the mutually agreed upon criteria. Unisys will notify the Service Desk that the move is complete via the "completed call" status entered in the SRMS/ServiceCenter system
- Complete the IMACD call ticket per the call closure procedures

Pricing for large-scale installation, move, add, and change projects, greater then 5 units will be agreed to during pre-project planning.

2.8.5 <DIR Customer> Obligations

<DIR Customer> will have the following obligations:

Providing work space consistent with <DIR Customer>'s space standards for Unisys and including a phone with voice mail, access to a data line, a locked space for tools, spare parts and storage of products, and access to buildings and Distributed IT Infrastructure.

Securing End-user device while in the possession of the End-user.

Providing consumable personal and network printer items such as paper, printer ribbons, toner and toner cartridges and for installation of such items as necessary.

Providing trash containers for the removal of packaging materials from <DIR Customer> Site.

Backing up End-user devices, laptop or notebook data. Providing all cable plants, cable termination device and cable inside building walls.

Providing designated disposal areas for all disposed devices.

Provide a site contact / coordinator at each site that receives the Services, The site contact / coordinator will have knowledge of the ITO statement of work and will provide support Unisys in the delivery of the Services.

2.9 Network Management

Note: Unisys will provide Network Management delivery based on the services as outlined in the Proposal

2.9.1 Monitor Service

Monitor Service primarily consists of Fault and Performance Management with web-based reporting. With Fault and Performance Monitoring, the MSC proactively monitors the client's network via a dedicated network connection with real-time detection of failures and performance threshold violations for managed network devices and primary interfaces that provide connectivity between managed network devices.

2.9.1.1 Real-Time Monitoring

In addition to receiving unsolicited SNMP traps that are sent from monitored devices, devices and managed interfaces are polled using HP Openview Network Node Manager. These status polls proactively monitor the managed network devices utilizing SNMP and ICMP. The default ICMP and SNMP parameters are:

- 5 minutes between polls
- Timeout of 0.8 seconds
- Two retries, if required, when the timeout interval is exceeded

These polling parameters are based on accepted best practices for network management. Due to ICMP limitations, false alerts may be generated for the managed devices. The MSC may have to adjust polling parameters to ensure delivery of ICMP Requests and reduce the number of false alerts.

2.9.1.2 Trouble Ticketing

The MSC utilizes event correlation to minimize unnecessary alarms and to quickly determine the root cause of the event. After a poll failure has been processed through the event correlation process, an audible and visual alarm is sent, via Unisys' Incident Management system, to the MSC. The Incident Management system contains all pertinent information relating to a particular device. Information includes points of contact, device location, service level agreements, and escalation procedures.

Trouble tickets generated are created with a severity of Critical, Warning, or Normal. Listed below are examples of events with the corresponding severity setting:

- Critical
- Root Cause Failure – Demand Poll Failure of Nodes
- Chassis Alarm – Fan Failure, Power Supply Failure, Temp. Warning
- Module Down
- The UPS is providing battery backup power
- Warning
- Server: Threshold exceeded – processor Utilization
- UPS on bypass
- Backup ISDN “Up” Status
- Server: Threshold exceeded – Free Memory Available is xxx
- Normal
- Cisco Cold Start
- APC UPS: Contact Normal
- Cisco Entity Reinitializing Itself
- Agent Threshold Resets

The MSC will notify the designated point of contact and provide a description of the problem and the trouble ticket number. The MSC will make three attempts to notify the client and will document each attempt in the trouble ticket. Notification will be accomplished by voice, email, or page.

The client will be able to view the trouble ticket via a secure web interface. This allows the client to keep informed, in near real-time, of all problem management activities and is the primary tool to use for status on problems.

2.9.1.3 Trouble Ticket Reporting

Trouble ticket reports are provided to the client on a regular basis via the secure website. Reports include monthly trouble ticket activity, monthly chronic problem report, and service level objectives. Reports are maintained for a thirteen-month time frame.

2.9.1.4 Monthly Trouble Ticket Activity

The monthly trouble ticket activity report will show the number of opened, closed, and backlog tickets for the previous month. There is also a summary and detail report for this category.

2.9.1.5 Monthly Chronic Problem Report

The monthly chronic problem report will identify any device that has had three or more outages during the previous 30 days.

2.9.1.6 Service Level Objectives Report

The monthly service level objectives report will show the number of events that meet or miss contracted Service Level Agreements (SLA).

2.9.1.7 Real-Time Monitoring – Traps, Thresholds, and Performance Reports

In addition to the serious events outlined in the section, several traps and thresholds are also monitored. The following table illustrates the typical traps, thresholds, and performance reports for MSC certified network devices. These parameters will vary by device. Unisys will review the specifics with the client during the transition phase.

Description	Relational Operator	Trap / Threshold	Event	Report
Device CPU Utilization	GE	50%	♦	♦

Device Memory Available	LE	1.25 MB	♦	♦
LAN Interface Utilization	GE	50%		♦
WAN Interface Input Utilization	GE	60%		♦
Wan Interface Output Utilization	GE	60%		♦
Interface Input Errors	GE	0.5%		♦
Interface Output Errors	GE	0.5%		♦
Interface Input Discards	GE	1%		♦
Interface Output Discards	GE	1%		♦
Ethernet Utilization	GE	10%		♦
Ethernet Collisions	GE	10%		♦
Ethernet Short Errors	GE	10%		♦
Ethernet CRC & Long Errors	GE	1%		♦
Ethernet Broadcasts	GE	50/sec		♦
Ethernet Multicasts	GE	100/sec		♦

GE = Greater Than or Equal To
LE = Less Than or Equal To

In addition to standard MIBII traps and thresholds, vendor specific MIBs are used to set additional performance traps and thresholds. During the first 90 days of operations management, the MSC will reevaluate the established trap and threshold criteria with the client for any required adjustments.

Reports are delivered to the client via a secure web server and are categorized as either exception or performance report. Reports are maintained for a thirteen-month time frame.

2.9.1.7.1 Exception Reporting

There are summary and detail exception reports that can be viewed by day or month. The Exception Summary reports describe exceptions to established thresholds with parameters that describe the exception. Exception Detail reports provide specific information on the device and correlated exception.

The following are examples of the Exception Detail reports:

- Router System Statistics – This report shows memory and buffer usage and items that are in the queue.
- Router CPU Utilization – This report shows the high, low, and average utilization for a router.
- Ethernet Segment Error Statistics – This report shows the “bad” frames that occur on a LAN segment that have exceptional behavior.
- Ethernet Utilization

2.9.1.7.2 Performance Reporting

Performance reports are categorized as daily and monthly. These reports are designed to cover all attributes that will assist the client in understanding performance and are broken down by device resources, device interfaces, LAN segments, and WAN links.

Daily and Monthly reports include:

- Network Availability/Delay Summary Report
- Network Availability Detail Reports
- Device Inventory Reports

- Inventory Detail Reports
- Protocol Statistics Detail Report – TCP/IP, DecNet, Appletalk, IPX, Bridged Traffic
- Total Traffic Detail Report – By device or segment

Monthly reports include:

- Device Total Traffic Report
- Ethernet Segment Health Summary Report – This report assigns a “health index” to the Ethernet segment by considering both the traffic and errors. The report shows a series of Ethernet segments with their respected health index
- WAN or LAN Health Summary Report - This report assigns a “health index” to specific interfaces on the managed routers to highlight situations that may require attention
- WAN Health Top 10 Report – This report builds upon the data presented in the WAN Health Summary Report and presents the Top 10 problem areas or “situations to watch”
- LAN Segment Health Top 10 Report – This report is similar to the WAN Top 10 report but is focused on identifying the Ethernet LAN segments that may require attention
- WAN and LAN Utilization Spectrograph Report – This report plots the utilization over time as percentages
- Trend Summary Report – This report presents a tabular view of key components and their projected progress into the near future
- Trend Detail Report – This report is derived from the Trend Summary Report and shows the underlying samples that contribute to the trend conclusions

2.9.1.8 Certification of New Devices

Before bringing new devices or modules into Remote Network Management Services, the MSC must validate that the device is currently certified in accordance with the MSC’s standards. If the device is not certified it must go through the MSC’s certification process, which includes:

- Evaluation of device manageability
- Evaluation of any element manager that may be required
- Evaluation of vendor support
- Testing of the device and any associated network management tools
- Analysis to determine critical parameters to monitor and establish default thresholds
- Definition, development and testing of performance reporting

In some cases the non-certified device may have manageability limitations or may be unmanageable. There may also be additional costs associated with the certification process. If it is mutually agreed to proceed, the MSC will provide a schedule for certification and transitioning of the new device(s) into production.

Upon completion of device certification, an addendum to this Statement of Work will be created for signature by the client that will describe the manageability level of the device and associated monthly management fees for the then remaining contract term. Once the addendum is executed by signature, the newly certified devices will be brought into remote management service.

2.9.2 Select Service

Select Service primarily consists of Fault, Performance, and Configuration Backup Management with web-based reporting. With Fault and Performance Monitoring, the MSC proactively monitors the client’s network via a dedicated network connection with real-time detection of failures and performance threshold violations for managed network devices and primary interfaces that provide connectivity between managed network devices.

2.9.2.1 Real-Time Monitoring

In addition to receiving unsolicited SNMP traps that are sent from monitored devices, devices and managed interfaces are polled using HP Openview's Network Node Manager. These status polls proactively monitor the managed network devices utilizing SNMP and ICMP. The default ICMP and SNMP parameters are:

- 5 minutes between polls
- Timeout of 0.8 seconds
- Two retries, if required, when the timeout interval is exceeded

These polling parameters are based on accepted best practices for network management. Due to ICMP limitations, false alerts may be generated for the managed devices. The MSC may have to adjust polling parameters to ensure delivery of ICMP Requests and reduce the number of false alerts.

2.9.2.2 Trouble Ticketing

The MSC utilizes event correlation to minimize unnecessary alarms and to quickly determine the root cause of the event. After a poll failure has been processed through the event correlation process, an audible and visual alarm is sent, via the Unisys Incident Management system, to the MSC. The Incident Management system contains all pertinent information relating to a particular device. Information includes points of contact, device location, service level agreements, and escalation procedures.

Trouble tickets generated are created with a severity of Critical, Warning, or Normal. Listed below are examples of events with the corresponding severity setting:

- Critical
- Root Cause Failure – Demand Poll Failure of Nodes
- Chassis Alarm – Fan Failure, Power Supply Failure, Temp. Warning
- Module Down
- The UPS is providing battery backup power
- Warning
- Server: Threshold exceeded – processor Utilization
- UPS on bypass
- Backup ISDN "Up" Status
- Server: Threshold exceeded – Free Memory Available is xxx
- Normal
- Cisco Cold Start
- APC UPS: Contact Normal
- Cisco Entity Reinitializing Itself
- Agent Threshold Resets

The MSC will notify the designated point of contact and provide a description of the problem and the trouble ticket number. The MSC will make three attempts to notify the client and will document each attempt in the trouble ticket. Notification will be accomplished by voice, email, or page.

The client will be able to view the trouble ticket via the secure web interface. This allows the client to keep informed, in near real-time, of all problem management activities and is the primary tool to use for statuses on problems.

2.9.2.3 Trouble Ticket Reporting

Trouble ticket reports are provided to the client on a regular basis via the secure website. Reports include monthly trouble ticket activity, monthly chronic problem report, and service level objectives. Reports are maintained for a thirteen-month time frame.

2.9.2.3.1 Monthly Trouble Ticket Activity

The monthly trouble ticket activity report will show the number of opened, closed, and backlog tickets for the previous month. There is also a summary and detail report for this category.

2.9.2.4 Monthly Chronic Problem Report

The monthly chronic problem report will identify any device that has had three or more outages during the previous 30 days.

2.9.2.5 Service Level Objectives Report

The monthly service level objectives report will show the number of events that meet or miss contracted Service Level Agreements (SLA).

2.9.2.6 Real-Time Monitoring – Traps, Thresholds, and Performance Reports

In addition to the serious events outlined in the section, several traps and thresholds are also monitored. The following table illustrates the typical traps, thresholds, and performance reports for MSC certified network devices. These parameters will vary by device. Unisys will review the specifics with the client during Implementation.

Description	Relational Operator	Trap / Threshold	Event	Report
Device CPU Utilization	GE	50%	♦	♦
Device Memory Available	LE	1.25 MB	♦	♦
LAN Interface Utilization	GE	50%		♦
WAN Interface Input Utilization	GE	60%		♦
Wan Interface Output Utilization	GE	60%		♦
Interface Input Errors	GE	1%		♦
Interface Output Errors	GE	1%		♦
Interface Input Discards	GE	1%		♦
Interface Output Discards	GE	1%		♦
Ethernet Utilization	GE	10%		♦
Ethernet Collisions	GE	10%		♦
Ethernet Short Errors	GE	10%		♦
Ethernet CRC & Long Errors	GE	1%		♦
Ethernet Broadcasts	GE	50/sec		♦
Ethernet Multicasts	GE	100/sec		♦

GE = Greater Than or Equal To
LE = Less Than or Equal To

In addition to standard MIBII traps and thresholds, vendor specific MIBs are used to set additional performance traps and thresholds. During the first 90 days of operations management, the MSC will reevaluate the established trap and threshold criteria with the client for any required adjustments.

Reports are delivered to the client via a secure web server and are categorized as either exception or performance report. Reports are maintained for a thirteen-month time frame.

2.9.2.6.1 Exception Reporting

There are summary and detail exception reports that can be viewed by day or month. The Exception Summary reports describe exceptions to established thresholds with parameters that describe the exception. Exception Detail reports provide specific information on the device and correlated exception.

The following are examples of the Exception Detail reports:

- Router System Statistics – This report shows memory and buffer usage and items that are in the queue.
- Router CPU Utilization – This report shows the high, low, and average utilization for a router.
- Ethernet Segment Error Statistics – This report shows the “bad” frames that occur on a LAN segment that have exceptional behavior.
- Ethernet Utilization

2.9.2.6.2 Performance Reporting

Performance reports are categorized as daily and monthly. These reports are designed to cover all attributes that will assist the client in understanding performance and are broken down by device resources, device interfaces, LAN segments, and WAN links.

Daily and Monthly reports include:

- Network Availability/Delay Summary Report
- Network Availability Detail Reports
- Device Inventory Reports
- Inventory Detail Reports
- Protocol Statistics Detail Report – TCP/IP, DecNet, Appletalk, IPX, Bridged Traffic
- Total Traffic Detail Report – By device or segment

Monthly reports include:

- Device Total Traffic Report
- Ethernet Segment Health Summary Report – This report assigns a “health index” to the Ethernet segment by considering both the traffic and errors. The report shows a series of Ethernet segments with their respected health index
- WAN or LAN Health Summary Report - This report assigns a “health index” to specific interfaces on the managed routers to highlight situations that may require attention
- WAN Health Top 10 Report – This report builds upon the data presented in the WAN Health Summary Report and presents the Top 10 problem areas or “situations to watch”
- LAN Segment Health Top 10 Report – This report is similar to the WAN Top 10 report but is focused on identifying the Ethernet LAN segments that may require attention
- WAN and LAN Utilization Spectrograph Report – This report plots the utilization over time as percentages
- Trend Summary Report – This report presents a tabular view of key components and their projected progress into the near future
- Trend Detail Report – This report is derived from the Trend Summary Report and shows the underlying samples that contribute to the trend conclusions

2.9.2.7 Fault Isolation

The MSC will use all available means to isolate the problem. This can include the use of an ISDN backup line, analog out-of-band connections, and network device diagnostics tools. After the problem has been isolated, the MSC will update the trouble ticket work-log with all pertinent information.
Out of Scope

2.9.2.8 Maintenance Dispatching

If the client has contracted for Unisys Infrastructure Maintenance Service for the managed network devices, the MSC will use the Unisys Incident Management system to electronically dispatch field engineers. Once on site, the field engineer will contact the MSC to coordinate restoration activities.

A Letter of Agency is required for devices that are maintained by third party vendors. The MSC will contact the respective service provider on behalf of the client with specific device information. If the third party service provider provides status updates, the MSC will document actions taken to resolve the problem in the trouble ticket work-log. The MSC does not manage third party SLAs.

2.9.2.9 Configuration Backup Management

If devices can have their configuration file remotely backed up, the MSC will backup the configuration file monthly or when the configuration file has been modified, and the client has notified Unisys of the modification. It is the client's responsibility to notify Unisys in advance prior to making any configuration changes. The MSC will verify the success and validity of each backup. The two most current configuration file backups are maintained for restoration purposes. The client retains ownership of the overall network design and configuration files for that design.

The MSC will maintain configuration information necessary to "roll back" to a previously known configuration state on a network element. This configuration will be provided to the client for implementation when roll back is required. The client is responsible for actually implementing the "roll back". The MSC can provide basic instructions, via phone, fax, or e-mail, for the re-installation of the configuration files.

2.9.2.10 Reviews

Unisys will conduct monthly status calls with the client to review the status of the remote network management program. This monthly review is intended to review and clarify any issues or areas of concern.

An in-depth Network Review will be conducted every [contracted time frame]. The MSC will review with the client a report that includes analysis of performance and fault activity during the previous reporting period and make recommendations to correct relevant critical areas of the managed network.

2.9.2.11 Certification of New Devices

Before bringing new devices or modules into Remote Network Management Services, the MSC must validate that the device is currently certified in accordance with the MSC's standards. If the device is not certified it must go through the MSC's certification process, which includes:

- Evaluation of device manageability
- Evaluation of any element manager that may be required
- Evaluation of vendor support
- Testing of the device and any associated network management tools
- Analysis to determine critical parameters to monitor and establish default thresholds
- Definition, development and testing of performance reporting

In some cases the non-certified device may have manageability limitations or may be unmanageable. There may also be additional costs associated with the certification process. If it is mutually agreed to proceed, the MSC will provide a schedule for certification and transitioning of the new device(s) into production.

Upon completion of device certification, an addendum to this Statement of Work will be created for signature by the client that will describe the manageability level of the device and associated monthly management fees for the then remaining contract term. Once the addendum is executed by signature, the newly certified devices will be brought into remote management service.

2.9.3 SelectPlus Service

SelectPlus Service primarily consists of Fault, Performance, and Configuration Management with web-based reporting. With Fault and Performance Monitoring, the MSC proactively monitors the client's network via a dedicated network connection with real-time detection of failures and performance threshold violations for managed network devices and primary interfaces that provide connectivity between managed network devices.

2.9.3.1 Real-Time Monitoring

In addition to receiving unsolicited SNMP traps that are sent from monitored devices, devices and managed interfaces are polled using HP Openview's Network Node Manager. These status polls proactively monitor the managed network devices utilizing SNMP and ICMP. The default ICMP and SNMP parameters are:

- 5 minutes between polls
- Timeout of 0.8 seconds
- Two retries, if required, when the timeout interval is exceeded

These polling parameters are based on accepted best practices for network management. Due to ICMP limitations, false alerts may be generated for the managed devices. The MSC may have to adjust polling parameters to ensure delivery of ICMP Requests and reduce the number of false alerts.

2.9.3.2 Trouble Ticketing

The MSC utilizes event correlation to minimize unnecessary alarms and to quickly determine the root cause of the event. After a poll failure has been processed through the event correlation process, an audible and visual alarm is sent, via the Unisys Incident Management system, to the MSC. The Incident Management system contains all pertinent information relating to a particular device. Information includes points of contact, device location, service level agreements, and escalation procedures.

Trouble tickets generated are created with a severity of Critical, Warning, or Normal. Listed below are examples of events with the corresponding severity setting:

- Critical
- Root Cause Failure – Demand Poll Failure of Nodes
- Chassis Alarm – Fan Failure, Power Supply Failure, Temp. Warning
- Module Down
- The UPS is providing battery backup power
- Warning
- Server: Threshold exceeded – processor Utilization
- UPS on bypass
- Backup ISDN "Up" Status

- Server: Threshold exceeded – Free Memory Available is xxx
- Normal
- Cisco Cold Start
- APC UPS: Contact Normal
- Cisco Entity Reinitializing Itself
- Agent Threshold Resets

The MSC will notify the designated point of contact and provide a description of the problem and the trouble ticket number. The MSC will make three attempts to notify the client and will document each attempt in the trouble ticket. Notification will be accomplished by voice, email, or page.

The client will be able to view the trouble ticket via the secure web interface. This allows the client to keep informed, in near real-time, of all problem management activities and is the primary tool to use for statuses on problems.

2.9.3.3 Trouble Ticket Reporting

Trouble ticket reports are provided to the client on a regular basis via the secure website. Reports include monthly trouble ticket activity, monthly chronic problem report, and service level objectives. Reports are maintained for a thirteen-month time frame.

2.9.3.3.1 Monthly Trouble Ticket Activity

The monthly trouble ticket activity report will show the number of opened, closed, and backlog tickets for the previous month. There is also a summary and detail report for this category.

2.9.3.3.2 Monthly Chronic Problem Report

The monthly chronic problem report will identify any device that has had three or more outages during the previous 30 days.

2.9.3.3.3 Service Level Objectives Report

The monthly service level objectives report will show the number of events that meet or miss contracted Service Level Agreements (SLA).

2.9.3.4 Real-Time Monitoring – Traps, Thresholds, and Performance Reports

In addition to the serious events outlined in the section, several traps and thresholds are also monitored. The following table illustrates the typical traps, thresholds, and performance reports for MSC certified network devices. These parameters will vary by device. Unisys will review the specifics with the client during Implementation.

Description	Relational Operator	Trap / Threshold	Event	Report
Device CPU Utilization	GE	50%	♦	♦
Device Memory Available	LE	1.25 MB	♦	♦
LAN Interface Utilization	GE	50%		♦
WAN Interface Input Utilization	GE	60%		♦
Wan Interface Output Utilization	GE	60%		♦
Interface Input Errors	GE	1%		♦
Interface Output Errors	GE	1%		♦
Interface Input Discards	GE	1%		♦
Interface Output Discards	GE	1%		♦

Ethernet Utilization	GE	10%		♦
Ethernet Collisions	GE	10%		♦
Ethernet Short Errors	GE	10%		♦
Ethernet CRC & Long Errors	GE	1%		♦
Ethernet Broadcasts	GE	50/sec		♦
Ethernet Multicasts	GE	100/sec		♦

GE = Greater Than or Equal To
LE = Less Than or Equal To

In addition to standard MIBII traps and thresholds, vendor specific MIBs are used to set additional performance traps and thresholds. During the first 90 days of operations management, the MSC will reevaluate the established trap and threshold criteria with the client for any required adjustments.

Reports are delivered to the client via a secure web server and are categorized as either exception or performance report. Reports are maintained for a thirteen-month time frame.

2.9.3.4.1 Exception Reporting

There are summary and detail exception reports that can be viewed by day or month. The Exception Summary reports describe exceptions to established thresholds with parameters that describe the exception. Exception Detail reports provide specific information on the device and correlated exception.

The following are examples of the Exception Detail reports:

- Router System Statistics – This report shows memory and buffer usage and items that are in the queue.
- Router CPU Utilization – This report shows the high, low, and average utilization for a router.
- Ethernet Segment Error Statistics – This report shows the “bad” frames that occur on a LAN segment that have exceptional behavior.
- Ethernet Utilization

2.9.3.4.2 Performance Reporting

Performance reports are categorized as daily and monthly. These reports are designed to cover all attributes that will assist the client in understanding performance and are broken down by device resources, device interfaces, LAN segments, and WAN links.

Daily and Monthly reports include:

- Network Availability/Delay Summary Report
- Network Availability Detail Reports
- Device Inventory Reports
- Inventory Detail Reports
- Protocol Statistics Detail Report – TCP/IP, DecNet, Appletalk, IPX, Bridged Traffic
- Total Traffic Detail Report – By device or segment

Monthly reports include:

- Device Total Traffic Report

- Ethernet Segment Health Summary Report – This report assigns a “health index” to the Ethernet segment by considering both the traffic and errors. The report shows a series of Ethernet segments with their respected health index
- WAN or LAN Health Summary Report - This report assigns a “health index” to specific interfaces on the managed routers to highlight situations that may require attention
- WAN Health Top 10 Report – This report builds upon the data presented in the WAN Health Summary Report and presents the Top 10 problem areas or “situations to watch”
- LAN Segment Health Top 10 Report – This report is similar to the WAN Top 10 report but is focused on identifying the Ethernet LAN segments that may require attention
- WAN and LAN Utilization Spectrograph Report – This report plots the utilization over time as percentages
- Trend Summary Report – This report presents a tabular view of key components and their projected progress into the near future
- Trend Detail Report – This report is derived from the Trend Summary Report and shows the underlying samples that contribute to the trend conclusions

2.9.3.5 Fault Isolation

The MSC will use all available means to isolate the problem. This can include the use of an ISDN backup line, analog out-of-band connections, and network device diagnostics tools. After the problem has been isolated, the MSC will update the trouble ticket work-log with all pertinent information.
Out of Scope

2.9.3.6 Maintenance Dispatching

If the client has contracted for Unisys Infrastructure Maintenance Service for the managed network devices, the MSC will use the Unisys Incident Management system to electronically dispatch field engineers. Once on site, the field engineer will contact the MSC to coordinate restoration activities.

A Letter of Agency is required for devices that are maintained by third party vendors. The MSC will contact the respective service provider on behalf of the client with specific device information. If the third party service provider provides status updates, the MSC will document actions taken to resolve the problem in the trouble ticket work-log. The MSC does not manage third party SLAs.

2.9.3.7 Restoration

Unisys will manage service restoration of a device to an operationally ready level. The MSC will methodically isolate the problem to determine the required actions to restore service and initiate those actions; this may include a reboot of the device, a restoration of the previous configuration file, or a tactical configuration change. The MSC will further analyze the problem to determine the root cause of the problem.

Unisys will use the following tests to verify the device is restored to its operational state.

Device Class	Restoration Definition
Routers	Device is reachable from the MSC All managed interfaces are Administratively Up Packets can be sent and received over interfaces Agent is running and, if applicable for both MIBII and vendor MIBs, supports SNMP “gets” Telnet is functioning Excessive circuit errors, such as CRC errors, have not exceeded previously established thresholds

LAN Switches/Hubs	Device is reachable from the MSC Managed LAN interfaces are Administratively Up Agent is running and, if applicable for both MIBII and vendor MIBs, supports SNMP “gets” Telnet is functioning
CSU/DSU	Device is reachable from the MSC Agent is running and, if applicable for both MIBII and vendor MIBs, supports SNMP “gets”
UPS	Device is reachable from the MSC Agent is running and, if applicable, supports SNMP “gets”

For critical network elements, Unisys recommends out-of-band access is available for isolation and resolution.

2.9.3.8 Configuration File Backups

If devices can have their configuration file remotely backed up, the MSC will backup the configuration file monthly or when the configuration file has been modified. The MSC will verify the success and validity of each backup. The two most current configuration file backups are maintained for restoration purposes.

2.9.3.9 Configuration Management

Unisys will monitor and document any changes made to the configuration of the managed network device. Changes will be documented either in the work-log of the trouble ticket or MAC ticket. All changes are accomplished with the client’s approval and per the pre-approved change management process. The client retains ownership of the overall network design and configuration files for that design, with Unisys maintaining the passwords for the network devices. To request configuration changes, a MAC Request must be submitted at least 72 hours prior to the scheduled change. Upon acceptance of the MAC Request, the following outlines a process flow for updating / changing device configurations:

- MSC performs a risk analysis to determine possible impact
- MSC prepares the network and management structure
- MSC temporarily removes device and any downstream devices from active management
- MSC makes changes
- MSC performs verification of service and manageability of the device(s)
- Device(s) and any downstream devices are placed back into active management
- MSC notifies the client the change has occurred

2.9.3.10 Reviews

Unisys will conduct monthly status calls with the client to review the status of the remote network management program. This monthly review is intended to review and clarify any issues or areas of concern.

An in-depth Network Review will be conducted every [contracted time frame]. The MSC will review with the client a report that includes analysis of performance and fault activity during the previous reporting period and make recommendations to correct relevant critical areas of the managed network.

2.9.3.11 Move, Add & Change Request and Reports

The client may request moves, adds, and/or changes to the managed environment with the submission of a Move, Add & Change (MAC) ticket via the secure web server. MACs will be

processed per a mutually agreed to date and time between 72 hours and two weeks of acceptance by the MSC.

MAC Requests are limited to [5%] per month of the total number of contracted devices. This [5%] is based on the number of devices that are involved with individual MAC Requests during that month. If this percentage is exceeded, there will be additional MAC processing charges, minimally $270.00 per additional MAC. A MAC Request will be reviewed for complexity. MAC Requests that are complex in nature, involve more than [5%] of the managed devices, or affect the complete network environment will be deemed a project. The MSC will notify the client if a MAC Request is deemed a project. MAC Requests that are deemed a project are subject to additional charges for project management, network consulting, and implementation.

The MSC will coordinate with the client any physical MAC activity that involves Unisys onsite activities and/or third party maintenance for managed devices. Unisys onsite activities must be covered by an existing contract or there will be additional charges. A letter of agency will be required to coordinate activities with third-party maintenance providers.

MAC activity reporting is provided on a monthly basis via the client's secure web server. Two reports are available: Move / Add / Change Detail Report and Move / Add / Change Summary Report.

The Move / Add / Change Detail Report is a composite listing of tickets that have been created, are in progress, or closed for that particular month.

The Move / Add / Change Summary Report is based on the information reported in the detail report with a graphical display of the activity.

2.9.3.12 Certification of New Devices

Before bringing new devices or modules into Remote Network Management Services, the MSC must validate that the device is currently certified in accordance with the MSC's standards. If the device is not certified it must go through the MSC's certification process, which includes:

- Evaluation of device manageability
- Evaluation of any element manager that may be required
- Evaluation of vendor support
- Testing of the device and any associated network management tools
- Analysis to determine critical parameters to monitor and establish default thresholds
- Definition, development and testing of performance reporting

In some cases the non-certified device may have manageability limitations or may be unmanageable. There may also be additional costs associated with the certification process. If it is mutually agreed to proceed, the MSC will provide a schedule for certification and transitioning of the new device(s) into production.

Upon completion of device certification, an addendum to this Statement of Work will be created for signature by the client that will describe the manageability level of the device and associated monthly management fees for the then remaining contract term. Once the addendum is executed by signature, the newly certified devices will be brought into remote management service.

2.10 Distributed Systems Management

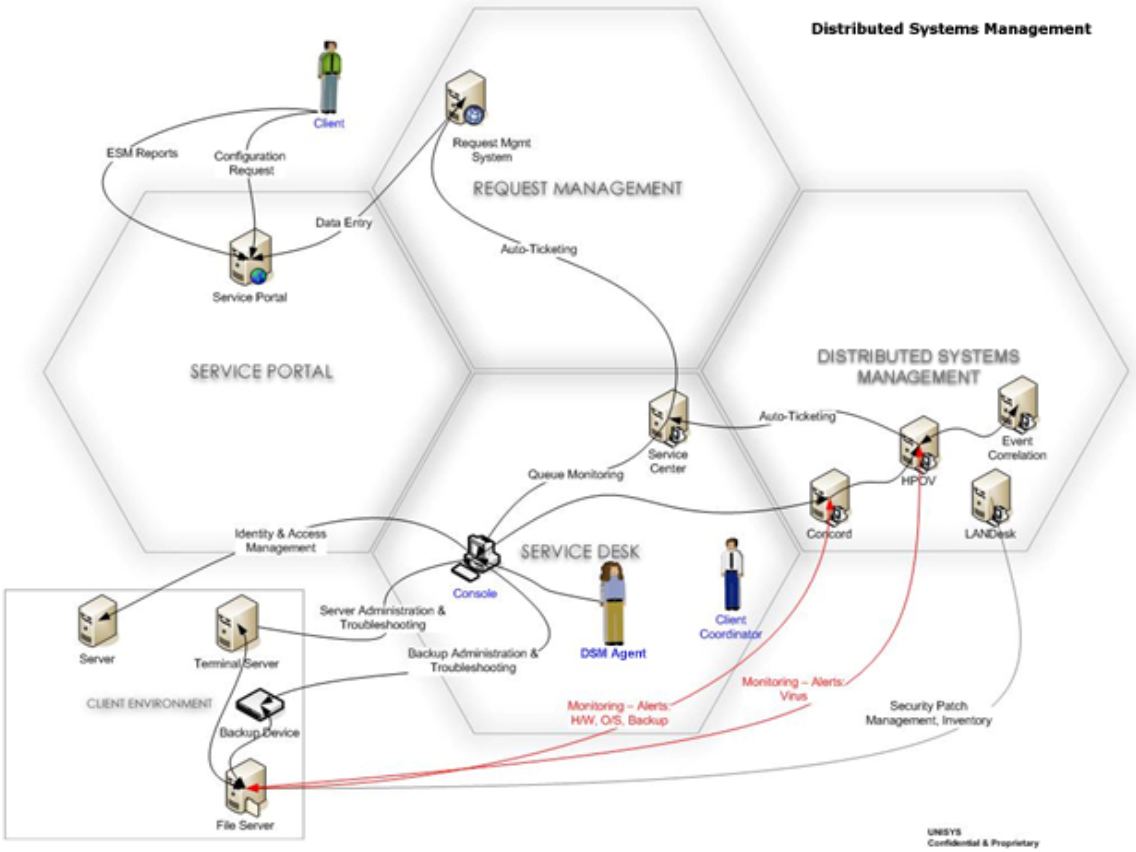
Distributed Systems Management includes all operational service delivery and support functions to ensure the availability of critical business applications in relation to server IT resources. Unisys

is authorized by <DIR Customer> to step into their existing system infrastructure and assume management of the servers that <DIR Customer> has negotiated.

2.10.1 Distributed Systems Management Service

Distributed Systems Management (DSM) provides holistic management and administration of the Distributed Systems Management (DSM) infrastructure as it relates to managed servers in a distributed homogenous environment (non-hosted).

The graphic below is a high-level overview of DSM:



2.10.1.1 Automated Server Monitoring and Resolution

Server monitoring is the process of reacting to automated faults generated and then troubleshooting and resolving the alerts either remotely or via dispatch onsite. Monitored aspects include system/network/OS/hardware level. This service focuses on monitoring against pre-defined thresholds, to ensure that the servers are functioning, available and performing well on the network and alerting the appropriate personnel of any issues or events.

2.10.1.2 Identity and Access Management

Identity and access management provides appropriate access to enterprise information and technology resources. This includes user account provisioning and user access control to various NOS platforms and server systems (email, Web, applications).

2.10.1.2.1 Authentication Management

Unisys will perform Authentication (Password) Management, which includes performing secondary password administration functions when the Service Desk is unable to perform password resets, the maintenance of password configuration and security settings.

2.10.1.2.2 Resource Management

Unisys will perform Resource management, which includes adding and deleting groups, adding and deleting group members, adding and deleting printer or file shares, and adding group permissions to and deleting group permissions from file or printer shares. Also included is the monitoring of the printing queues across a distributed environment.

2.10.1.3 Server Administration

Server administration activities include various tasks required to maintain the operational configuration for a given server or groups of servers within <DIR Customer>'s enterprise. These activities include general functional printing administration, managing server standardization, and enterprise server administration: WINS, DNS, and DHCP. These tasks provide the core for server configuration management.

2.10.1.3.1 Account Administration

Unisys will perform Account Management, which is the function of User Administration; administering network user accounts for new users and existing users and providing authorized access to network resources as directed by <DIR Customer>. Also includes performing file and directory security administration.

2.10.1.3.2 Directory Services Management

Directory Services Management & Administration services includes, but not limited to the maintenance and health of the following: WINS, DNS, DHCP, and Active Directory (AD) for a Microsoft environment and Network Directory Services (NDS) for a Novell environment.

2.10.1.3.3 Network Address Administration

Network address administration includes managing and administering the IP addresses of all servers in scope. Unisys will strictly follow the Systems Management Change Management process when making any changes to <DIR Customer>'s directory services or a network IP address.

2.10.1.3.4 Web Server Administration

Web Server Administration is the management of the enterprise web system. For web server applications besides Microsoft IIS (Linux Apache, Sun iPlanet) it must be determined whether Unisys has certified the application. On certified applications, Unisys will perform the following functions: Starting and stopping sites, restarting the web service, and changing the inherited defaults.

2.10.1.3.5 Proactive Server Management

Proactive Server Management ensures the enterprise server environment remains operational. Unisys will perform the services that include certifying, packaging, and documenting the distribution process that ensures standards are met and availability integrity is maintained for all server devices under this contract. Unisys will strictly follow the Systems Management Change Management process when making any changes to <DIR Customer>s server enterprise. All changes for servers will be maintained in a server configuration library.

2.10.1.4 Server Security Patch Management

Patch Management is the life cycle management process of applying security patches to server operating systems, which focus' on Microsoft security bulletins.

2.10.1.5 Server Anti-Virus Management

Anti-Virus Management is managing the deployment and use of virus management tools and updates, as well as assisting in removal of viruses when required. Unisys will adhere to the agreed upon virus protection processes, procedures, tool-sets, and standards. The Systems Management team will ensure that the agreed current version of the virus protection software is deployed to all desktops and servers. As new updates are received the Systems Management team will validate the updates and complete the appropriate actions to maintain the integrity of the enterprise environment. In the event a virus Incident occurs Unisys will provide the appropriate support and problem management activities to manage, contain and resolve the situation. This includes communications to end-users via e-mail and/or web on virus policies and virus Incident news and procedures.

2.10.1.6 Server Backup and Restore Management

Backup and Restore Management, which provides server continuity management, is managing and monitoring enterprise server back-ups to tape or other media, the daily administration required for backup and restore management, and performing server data restores when recovering from an isolated server failure.

2.10.1.6.1 Backup Archival and Retention

Unisys will manage the Backup Archival and Retention process of server backup tapes.

2.10.1.6.2 Restore

Unisys will manage restores for the purpose of recovering a server or solving a problem on a server. The Systems Management Team will provide individual file restores to servers in situations where the file is the cause of a problem affecting the performance of a server or application running on that server.

2.10.1.6.3 Daily Administration

Unisys will monitor the completion status of all scheduled and managed backups to ensure that the backup completed successfully. Unisys will perform a full/complete or incremental backup per managed server per the agreed upon backup procedure. If a backup does not complete successfully, Unisys will investigate the reasons for non-completion, identify and implement the appropriate actions to either re-start or complete the job successfully. If any of these activities require manual intervention at the local server, the Systems Management team will interface with the designated <DIR Customer> site contact and/or the Unisys Program Office to ensure that these activities are undertaken and completed as required.

2.10.1.7 DSM Service Processes

The following processes are utilized in providing Distributed Systems Management.

2.10.1.7.1 Incident and Problem Management

The Unisys Service Desk will be responsible for all <DIR Customer> end user support as related to the Systems Management service. All services impacting <DIR Customer> systems will be reviewed and prioritized to focus on meeting <DIR Customer> SLAs and business priorities. The Service Desk will provide to the entitled <DIR Customer> user an Incident ticket Request number. If the Service Desk cannot remedy the Incident Request, and the Request is identified as a Systems Management issue, the Service Desk will process the Incident Request to the designated Systems Management team for Incident resolution. The System Management team will prioritize Incidents to meet business objectives in accordance with contracted SLA's and business requirements. See Service Desk with Request Management in this document for a detailed description of the Service Desk processes.

When the Service Desk identifies multiple like Incidents or a major Incident for which they do not have a permanent solution, they will be moved to the Problem Management team for resolution. The Service Desk has responsibility to manage and update the Configuration Management Database (CMDB) so that once a resolution is determined; the Service Desk can perform the required solution the next time the Incident occurs.

2.10.1.7.2 Configuration Management

Service Delivery Data Management (SDDM) is the Configuration model (version of configuration management) that Unisys has adapted to support DSM services. SDDM allows the identification, control, maintenance and verification of devices existing in <DIR Customer>'s environment. SDDM includes the following:

- Define a limited set of requirements and processes to track, manage and leverage device/asset data within the DSM solution model
  - Unisys may use external partners to provide supplemental resources, based on the requirements determined for <DIR Customer>
- Perform inventory collection services for all specified locations to identify and asset tag all devices/assets designated to be covered under this DSM contract
- Define and document steady state procedures to be followed by Unisys and <DIR Customer> to ensure the accurate tracking and update of device/asset information

To ensure the best possible outcome for a successful SDDM startup and inventory, <DIR Customer> needs to provide to Unisys certain items that are uniquely under the control of <DIR Customer>.

Steady-State responsibilities will include, coordination of data updates to the Unisys repository through the IMACD process, communication with <DIR Customer> as an escalation point when failures are identified, coordinating or performing support as they align to original project goals as necessary.

2.10.1.7.3 Change Management

Unisys will utilize a formal change control process which allows accurate tracking and approvals for any changes to the scope of work beyond day to day operations. This covers server additions and deletions from the network, new sites, directory services design and all other items not specifically covered by this Statement of Work.

2.10.1.7.4 Release Management

The following processes have been created to control the release of software and hardware into <DIR Customer>'s environment.

2.10.1.7.4.1 Software Release Management

The following process is used to release new software or patches into the client's environment:

- Identification - Identification of the software or patches to be installed
- Discover - Inventory of servers to determine which shall receive the software or patches
- Testing - A critical component of Unisys' release strategy is the testing process. Prior to deploying any systems updates, Unisys undertakes a thorough analysis of system configuration changes that will take place and ensures that impacts, dependencies and risks are completely modeled. Unisys will then validate the updates in a lab environment. The complexity of the testing will depend on the level of complexity of <DIR Customer>'s server enterprise.
- Scheduling - Create a policy that assigns the updates or installation to a target group and monitor for issues and success

- Executing - Once an update has been thoroughly evaluated and dependencies are understood, Unisys schedules the distribution of the update. The process will monitor the distribution success using the Web Portal interface. If a server requires a roll-back, Unisys will take the necessary corrective actions.
- Validating - Provide drilldown reporting on the software release project

2.10.1.7.4.2 Hardware Release Management

The following process is used to release new hardware styles into the client's environment:

- Procure new hardware - <DIR Customer> procures the hardware device (If <DIR Customer> has purchased provisioning, Unisys will procure)
- Testing - Unisys will set up new hardware in the <DIR Customer> provided lab environment and load <DIR Customer> supplied software applications for testing
- Scheduling - Unisys will work with <DIR Customer> to schedule the installation of the new device into the <DIR Customer>'s environment and test with a target group
- Release - Upon the successful evaluation of the hardware in a target group, the hardware will be scheduled for release into the <DIR Customer>'s environment
- Validation - Monitoring and reporting on the operation of the new device

2.11 Security Management Services

Unisys will provide Network Management delivery based on the services as outlined in the Proposal

Network Security Services

2.11.1.1 Network Firewall and VPN

Unisys will provide Network Management delivery based on the services as outlined in the Proposal

2.11.1.2 Intrusion Detection and Prevention

Unisys will provide Network Management delivery based on the services as outlined in the Proposal

2.11.1.3 Security Remote Access

Unisys will provide Network Management delivery based on the services as outlined in the Proposal

2.12 Software Licenses

<DIR Customer> will purchase and maintain, at its own expense, all software licenses and agents used in providing Services under this Statement of Work that resides on <DIR Customer> owned products.

Unisys will purchase and maintain, at its own expense, all software licenses and agents used in providing Services under this Statement of Work that resides on the Unisys owned products.

3 Program Management Office – Governance

The Unisys Program Management Office (PMO) provides the management structure and ancillary support services, including Operations management, Service Delivery management, administrative functions (billing, expenses, time tracking, reporting, etc) and provisioning support as well as matrix management for all remotely delivered services including Single Point of Contact Service Desk, System Management, Managed Security, etc.

Under the direction of the Unisys Account Manager (UAM), the Unisys PMO will provide the following:

3.1 Continuous Service Improvement Process

Unisys utilizes a layered approach to Continuous Improvement (CI). At a customer/account specific level Unisys utilizes a Continuous Service Improvement Process (CSIP), which provides the necessary tools, authority, and accountability to drive CI for the account by the PMO. On a broader level Unisys utilizes the ITO Continuous Improvement Process (ICIP) to drive CI across all our accounts, sharing best practices, lessons learned, etc.

3.2 Unisys Operations Team

The implementation team will turn over primary responsibility to the operations team, or Program Management Office at Go-Live. The Program Management Office is managed by the Unisys Account Manager who will be the primary Unisys representative under this SOW. The Account Manager will have overall responsibility for managing and coordinating the performance of Unisys obligations and is authorized to act for and on behalf of Unisys with respect to all service delivery matters. The Account Manager will be the point of contact for <DIR Customer>'s appointed Program Manager.

The Unisys Operations Manager monitors day-to-day operations and coordinates with the client and Unisys Service organizations to ensure delivery of all services as defined under this SOW.

3.3 Communication

3.3.1 Monthly Status Review Meetings and Reports

The UAM will schedule joint communication and status review meetings to be held at least monthly with the <DIR Customer> PM. The purpose of these meetings will be to communicate program status and address program issues.

Unisys will provide the <DIR Customer> PM with written status reports as described in the Appendix F.

Service Desk End User Guide
Unisys will publish and maintain an End User Guide based on mutually agreed to update and maintenance processes. The guide will be maintained in electronic form on the <DIR Customer> intranet. Unisys will maintain the End User Guide so that it reflects any updates to the information provided in previous guides.

3.3.2 Customer (End User) Satisfaction Surveys

End User or Customer Satisfaction is the key metric for measuring the value and quality of a Service Desk and initiating the continuous improvement cycle. Throughout the term of this ITO SOW, Unisys will contact the End User to conduct a satisfaction survey. Unisys conducts point-of-service surveys via phone to measure the qualitative elements of the service delivery. The standard Unisys format, a seven question survey, will be used and will be conducted on approximately 10% of the Survey-able Service Desk calls closed by the Service Desk for the past month. These surveys are performed by the Unisys ISO9000 survey team.

The Unisys Service Desk survey is tailored to define ongoing customer satisfaction with specific service attributes. These results are also an integral part of Service Desk agent employee and departmental performance objectives. The survey requests that the end user rates performance for call responsiveness, Incident resolution time, Incident resolution quality, service orientation, and overall satisfaction. The survey results are then used in the continuous improvement process.

If a survey response indicates a low satisfaction rating, corrective action is taken resulting in s either process improvements, additional training or technology changes. When the survey results indicate high customer satisfaction, the situation is reviewed to replicate the process that resulted in exceptional service. The surveys will commence in the second month of Operations and continue through the term of this SOW. The survey results, along with the associated raw data, will be reported monthly to <DIR Customer>.

3.4 Unisys Service Level Management

Each month Unisys will track and report performance against the Service Levels that are the subject of the Statement of Work. Such reports will show Unisys total performance, and highlight exceptions listing those tasks and metrics that do not meet the established Service Levels. The exception report will indicate Unisys corrective action plan for any Services not meeting the established Service Levels.

3.5 Strategic Quarterly Review

<DIR Customer> and Unisys will form a steering committee to facilitate executive-level communications between the parties (the “Steering Committee”). The Steering Committee shall be composed of the <DIR Customer> Program Manager, <DIR Customer> Chief Information Officer or his/her designee, the Unisys Account Manager, Unisys Executive Sponsor, and other persons as mutually agreed by the parties.

A quarterly formal management meeting (“Strategic Quarterly Review Meeting”) of the Steering Committee will be held at a mutually agreed location and time. The primary purpose of this meeting is to help align <DIR Customer> and Unisys relationship to <DIR Customer>’s strategic business and IT goals. The meeting agenda will be mutually agreed to, and may include the following topics:

- Review of the Reports for the quarter;
- Review of the overall performance of the Services by Unisys;
- Review of the progress of the resolution of previously discussed open issues
- Review of <DIR Customer>’s strategic business and IT goals, especially any changes since the previous Strategic Quarterly Review
- Discussion of other matters as mutually agreed by the parties

3.6 <DIR Customer> Site Meetings

On at least a quarterly basis the <DIR Customer> PM and Unisys AM will conduct meetings at a predefined mutually agreed upon <DIR Customer> Site. The purpose of such meetings is to provide communication to the <DIR Customer> Sites about the ITO Services and to elicit feedback from the <DIR Customer> Sites as to <DIR Customer>'s overall satisfaction with the program.

3.7 Project Management

The Unisys PMO will provide overall project management for all contracted project work during the period of this Statement of Work. If other Unisys or third parties are utilized by the PMO, the Unisys PMO will provide the top-level project management and will be <DIR Customer>'s single-point-of-contact.

3.8 <DIR Customer> Program Manager

<DIR Customer> will appoint a Program Manager who will serve as the primary representative for <DIR Customer> under this SOW. The <DIR Customer> PM will manage and coordinate <DIR Customer>'s performance under this SOW. The <DIR Customer> PM will render or obtain and implement in a timely manner all <DIR Customer> decisions required to permit Unisys to meet its responsibilities under this SOW.

4 Implementation

4.1 Five Stages of Implementation

The Implementation phase brings an ITO client from signed contract to Operations. It includes: Start-Up, Assessment, Comparison/Design and Transition, which leads to Operations.

A Unisys Transition Manager is assigned to lead the overall implementation, and each contracted ITO service also assigns an Implementation Manager/Subject Matter Expert (several services may be assigned to a single individual). Note that Implementation Manager and Subject Matter Expert (SME) will be used interchangeably in this document. The Transition Manager ensures that the implementation follows all of the Unisys project business practices. These practices are to ensure that the project delivers what is defined in this Statement of Work on time and at the agreed to prices. The prices are defined as implementation prices and operational prices. Both of these are defined in the pricing models delivered by the Engagement Manager during the Engagement to Implementation Turnover with the modifications made via change orders.

4.1.1 Start-Up

The ITO Transition Manager is assigned, and is supported by a team of subject matter experts. This Implementation Team meets with the <DIR Customer> Transition Manager and key <DIR Customer> personnel that will support the Implementation Project. During this part of the project, long lead-time items are addressed – this includes identifying Telecommunication needs, such as toll free or toll numbers and any data circuits to be ordered.

4.1.2 Assessment

The purpose of the Assessment Stage is to gather specific information about <DIR Customer>'s current IT Distributed Infrastructure Environment. Specific information is gathered about <DIR Customer>'s current systems, tools, procedures and any other data describing the objectives, needs and desires for the new, improved next generation and future state methods and practices. The Implementation team will also use the Assessment process to complete any due diligence that could not be completed during the Engagement Phase

In order to ensure that Unisys can efficiently gather accurate and timely data, <DIR Customer> will provide timely access to all individuals, documented processes, data and resources as defined in the Implementation Plan. The resources that are typically interviewed are:

- Chief Information Officer or organizational equivalent
- Security Officer and staff
- Help Desk Manager(s)
- Help Desk Analysts
- 2nd and 3rd level internal Support Personnel
- 2nd and 3rd level external Support Personnel
- Selected End-users
- Selected Business Unit Managers

Examples of the type of data required include:

- Desktop naming convention(s)
- Desktop/security policy
- Image Management
  - Number of core images
  - Tier/layering process
  - End user storage and “personalities”
- Current image and desktop management tools (e.g. Wise)
- For the most recent 3 month period
  - Total Calls to the help desk by month and daily
  - Total Tickets created by month and daily
  - Average handle time by month and daily
  - ACD call data by month and daily
  - Number of calls with detail referred to internal Level 2 support by month and daily
  - Number of calls with detail referred to external Level 2 support by month and daily
  - Call History Detail by month and weekly
- Call Flow Documentation
- Call Referral and Escalation Procedures
- Supported Products Information (Hardware and Software)
- Organization Charts
- Customer Satisfaction Survey Details
- Internal Help Desk Marketing Information (How to call, expectations, etc.)

Once the Assessment Report is completed, it will be provided to <DIR Customer>. <DIR Customer> and Unisys will review, make adjustments as necessary, and <DIR Customer> will provide written acknowledgement that the Assessment Report is complete and accurate.

4.1.3 Comparison / Design

The purpose of the Comparison process is to compare the findings from assessment against the assumptions made in the Statement of Work. If any of the findings differ significantly from the assumptions then changes must be made to either the current state to bring the item into compliance or the Statement of Work via a change order.

The Comparison process relies on the current state assessment report as a critical input. With the assessment report, the comparison process can begin with the goal of identifying discrepancies between the current state and the Statement of Work assumptions. Before beginning the Comparison process along with the deliverables from the previous processes being completed, the assessment report must also be completed and signed off by <DIR Customer>.

If there is a discrepancy between the findings of Assessment and the requirements and/or assumptions of the Statement of Work, then this must be documented in the Gap Register. The output of this process is the Gap Report which must be completed and receive sign-off from <DIR Customer>. This document will form the basis of design adjustments to the proposed solution. The Final Design Documents will detail the services provided, and must receive sign-off from <DIR Customer>.

4.1.4 Transition

The purpose of the Transition process is to install the solutions required to perform operations according to the Statement of Work. During the Transition process all systems must not only be installed but will also be tested as appropriate. All required staff will be hired and trained. The Service Desk will be fully functional.

This phase involves putting the design into action.

- Migration Planning – A step-by-step Project Plan is created to minimize client risk, and to allocate appropriate resources to the implementation project.
- Migration, Turn-Up, and Testing – the implementation of the Migration plan and service management, Service Delivery management, if equipment changes or client site visits are required. The result of this phase will be that the systems will be in place to provide the contracted services.
- Documentation Handoff – Any and all <DIR Customer> policies, procedures, and standards will be documented in the Policies, Procedures, and Standards Guide (PPS).

Approximately one week prior to the scheduled startup of operations a Readiness Review meeting is held. At this meeting, the <DIR Customer> Transition Manager and the Unisys Transition Manager must agree that everything is on schedule to Go-Live. Note: typically many items are not yet scheduled to be complete at this point – the review is to assess progress to date and remaining open items, not to determine that everything is already complete.

4.1.5 Operations

At Go-Live, the Implementation Team turns the primary responsibility over to the Operations Team, while continuing to monitor operations for approximately one month. During this process a final review is performed with the operations team and <DIR Customer> to clarify all the information required for operations.

This is the point where the day-to-day Unisys to Client relationship begins according to normal Unisys procedures, including the additional tasks of:

4.2 Critical Milestones

Milestone	Due Date	Responsible Party
Program Start Date	Contract	Unisys / <DIR Customer>
Assessment Complete	Start Date + 4 weeks	Unisys / <DIR Customer>
Gap Analysis Delivered	Data Collection complete + 2 weeks	Unisys

Initial Design Delivered	Gap Analysis complete + 2 weeks	Unisys
Readiness Review Meeting	Go-Live minus 1 week	Unisys / <DIR Customer>
Go Live	Design Acceptance + 7 weeks	<DIR Customer> / Unisys
Implementation Complete	Go Live + 2 weeks	Unisys / <DIR Customer>

4.3 Unisys Implementation Team

Unisys will assign an implementation team to implement the contracted services under this SOW. The implementation team is led by the Unisys Transition Manager who has the overall responsibility for the ITO Implementation and ensures that the services being implemented are as defined in the SOW. The implementation team will also have a Subject Matter Expert (SME) for each of the contracted services (several services may be assigned to a single individual).

5 Appendix A – Pricing Parameters

TO BE COMPLETED BASED UPON THE SERVICES THAT THE CUSTOMER CHOSES FROM THE PROPOSAL.

6 Appendix B – Definitions

TO BE COMPLETED BASED UPON THE SERVICES THAT THE CUSTOMER CHOSES FROM THE PROPOSAL

7 Appendix C – Roles and Responsibilities

TO BE COMPLETED BASED UPON THE SERVICES THAT THE CUSTOMER CHOSES FROM THE PROPOSAL and subsequent Joint Responsibility Matrix (JRM) will be developed

.

8 Appendix D – Change Management Process

TO BE COMPLETED BASED UPON THE SERVICES THAT THE CUSTOMER CHOSES FROM THE PROPOSAL

9 Appendix E – Service Level Agreement

TO BE COMPLETED BASED UPON THE SERVICES THAT THE CUSTOMER CHOSES FROM THE PROPOSAL

10 Appendix F – Standard Reports

TO BE COMPLETED BASED UPON THE SERVICES THAT THE CUSTOMER CHOSES FROM THE PROPOSAL

11 Appendix G – Supported Hardware

TO BE COMPLETED BASED UPON THE SERVICES THAT THE CUSTOMER CHOSES FROM THE PROPOSAL.